Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Information Security Management in France: Perceptions and Influence of Culture, Regulations

by

DIOP, MAME

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: 2007

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Information Security Management in France: Perceptions and Influence of Culture, Regulations

by

DIOP, Mame

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: 2007

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Information Security Management in France:

- Perceptions and Influence of culture, regulations

A Security Study

By

Mame G. DIOP

Year 2006/2007

ABSTRACT

Considering that many organizations today are fully dependent on information technology for survival, information security is one of the most important concerns facing the modern organization.

'Security can be complex as you enter the international arena. It is essential to take cultural differences into account while managing security in an international environment[1]' Paul Raines, Chief Information Security Officer, OPCW, United Nations

This study attempts to reveal some of the impact of culture, regulations on security approach; and also why a security certification is not well adopted in French companies in opposition to other countries like Japan or US. The central objective is also to give an answer to what many security professionals agree (or not) that culture and local rules/regulations are something we have to deal with in order to preserve security.

[1] http://www.forrester.com/events/agendabyday/print/0,9022,1471,00.html

1. Acknowledgements

I would like to express my gratitude to all those who gave me the possibility to complete this research. I want to thank the Faculty of Professional Education of the Concordia University college of Alberta.

I have furthermore to thank my two research advisors, Mr Ron Ruhl, Director of the Information Systems Security (ISS) Program and Mr Pavol Zavarsky, Director of Research. I want to thank them for their help, support, interest and valuable hints. I also want to thank Iain Kyte for his help and the ISSM research committee which allowed me to work on this topic.

Especially, I would like to give my special thanks to all the ISSM staff at Concordia (Judy Wach, Dale Lindskog, Andy Igonor, Ed Brownfield) for their support, the knowledge they gave me during my visit at Concordia.

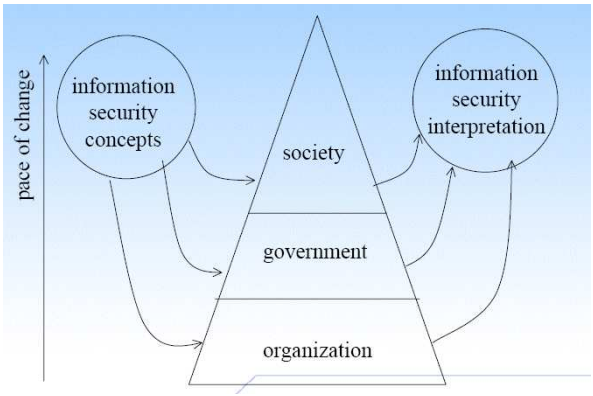
Great thanks to the security professionals that took the time to answer to the survey and thus gave valuable information to achieve the study.

2. Introduction

Complex information system security today focuses on the design of safe and secure information systems and their operations. However, the human factors must also be taken into account because technology alone cannot lead to an adequate solution.

The motivation behind this paper is related to the fact that France is one of the countries with the lowest number of ISO 27001 certificates compared to other countries like Japan, US and the UK. French security professionals point out many issues related to government bad security organization[2]: Pierre Labordes talks about *"the administrative disorder which represents French government action in terms of information security"*. But also, there is a lack of security maturity of companies and the influence of culture. The research aim is to understand the challenges in information security management specifically in relation to culture, laws and regulations in France. A qualitative method is used in this study to offer discussions, explanations and theoretical analysis.

According to a study of Tuija Helokunnas, September 25, 2003, Information security is interpreted via Culture. Information security concepts involving norms, standards, techniques and products conduct to information security interpretation via society, government and organization. Thus, this interpretation depends among other things on individuals values. In this study, we will explore culture in order to learn more about its influence on information security management in France, investigating French values, behavior and perceptions.



A complete definition of information security management is:
"Information Security Management is about the protection of information assets from potential security breaches. It starts with reviewing risks, setting policies, processes and controls, and by implementing them throughout the organization. Information Security Management relates to all types of information, be it paper-based, electronic or other. It determines how information is processed, stored, transferred, archived and destroyed." [3]

[2] Pierre Labordes is a French Deputy (a congressman) who did a study pointing out government disorder in terms of security, etc.

[3] http://www.saiglobal.com/assuranceservices/certification/InfoSecurityManagement/

In summary, Information Security Management is what any organization needs in its day-to-day operations to face actual and emerging threats. Many standards exist in this area, and one of them is BS 7799-1 or ISO 17799, a widely used British standard. "*ISO 17799 gave industry a framework for addressing all the management aspects of information security*" ISO Bulletin December 2000. ISO 17799 is a guide of security best practices that enables business to establish management systems in order to address among others: the organizational aspects, issues related to human resources, third party access, human resources, security responsibilities, legislative controls...It addresses the problem of how to ensure that information systems are managed and used in a secure way.

Then what became part 2 of BS 7799 has been improved and refined to ensure widespread practical application at international levels. ISO 27001 is actually globally recognized as the standard against which organizations can be certified in opposition to ISO 17799 which is just a Code of Practice. In France, LSTI is an independent company that delivers an ISO 27001 security certification. LSTI participates in the elaboration of norms at a national (within a French association called AFNOR[4]) and international (within ISO) levels. Its Chief Executive Officer (CEO), Ms Armelle Trotin was interviewed for the purpose of this study. Statistics about actual adoption of ISO 27001 can be found at: http://www.iso27001certificates.com/

Certification to ISO 27001 is a powerful step for an organization toward effecting and demonstrating compliance with other laws and standards like Sarbanes-Oxley and HIPAA. Once an organization is certified, it is globally accepted. The benefits are: credibility, trust, satisfaction and confidence with stakeholders, partners, citizens, customers. Having a security certification can at times create a market differentiation due to prestige and image. We remember the powerful effect that ISO 9000/4 had on quality assurance movement of the 1990s. Many countries including France adopt this certification; but apparently France didn't follow this trend with ISO 27001 if we look at the statistics.

After the previous introducing part about culture, information security management and ISO standards, this paper explores existing laws and regulations in France, Europe and other countries. The comparative exercise serves many purposes. Two of them are: foremost, to draw out the points of difference between information-privacy law in Europe, USA and Japan; differences that can be explained by culture. Then, to attest that there is in France, no existing law or regulation related directly or indirectly to information security management.

Beyond this comparison, two models of cultures dimensions studied by Geert Hofstede′s and Edward T. Hall′s and general statements about culture are presented. Both models will help provide a framework to use to examine the cultural context of security practices.

The rest of this paper is organized namely: In the first part, collected data about French laws and regulations in French companies, opinions about influence of culture are discussed. The collection of data was done during phone interviews and, questionnaires which were sent electronically. This is followed by an analysis of the factors that hold back the adoption of a security standard like ISO 27001. The third part attempts to do a theoretical analysis to explore security organization in different countries, to explain the role of culture in this context and to define some ways to improve security management.

4 AFNOR Group: A Group which has demonstrated its expertise in four complementary activities: standardization, training, certification, publication and distribution of information products

3. Laws and Regulations

3.1. French laws/regulations related to ISS

The French government website dedicated to information systems security: http://www.ssi.gouv.fr/en/index.html lists existing laws and regulations. This section presents a survey of the French legal context:

Related to	Content
Cryptology	According to article 30-I law 2004-575 June 21st 2004, using crypto means is free. Providing, importing and exporting cryptology are regulated in France. The Central Directorate for Information Systems Security (DCSSI) records declarations and investigates requests for the authorization of cryptology equipment and services in accordance with French and community legislation.
Evaluation and certification	The Central Directorate for Information Systems Security (DCSSI) is responsible for examining certifications according to the directives given by the certification management committee. Certification is based on evaluation studies conducted by laboratories licensed by the French Prime minister and accredited by the French accreditation committee (COFRAC). ISO 15408 is used as a reference to evaluate and certify the security of IT products and services.
Information systems	Directive relating to the physical protection of information on protected supports also the protection of national defense secret.
Compromising signals	Directives related to installation rules for sites and systems dealing with sensitive information not governed by defense secrecy.
Methods used to achieve information systems security in France	*EBIOS* (Expression of Needs and Identification of Security Objectives): a method used to assess and treat risks relating to information systems security (ISS). *PSSI* (Information Systems Security Policy): provided ISS managers with a framework for preparing an information systems security policy in their organization. *TDBSSI* (Information Systems Security Trend Chart): An ISS trend chart is a management tool used at various levels of decision-making, management, and operations.

3.2. European regulations related to ISS

France as part of the European Union (EU) is under some regulations defined by competent authorities. So, this section presents some directives with regard to consumer protection, personal data protection, electronic signatures, etc.

3.2.1.Personal data protection

Europe has proven to be the leader in protecting the privacy of the individual in the digital age. The privacy issue is particularly relevant to Europe. But US observers look toward the EU provisions with admiration and hope that Americans will see fit to adopt at least some of the philosophy of protecting consumers against privacy invasions to data[5]:

- *The Council of Europe*[6] set out various basic privacy principles and provided a template for countries without data protection legislation. So, the Council ended up with the foundation of subsequent privacy regulation in Europe. And to well manage and protect data flows between the EU and other jurisdictions, the Organization of Economic Co-Operation and Development (OECD[7]) was created in 1981.

- *OECD*'s guidelines aim at harmonizing national privacy legislation and providing a framework for facilitating the international flow of data. It represents the first trans-Atlantic agreement relating to privacy protection.

- *The EU Privacy Directive* was established in 1998 to increase data privacy protection within the European Union and to be an integrated part of EU policy. This will help promoting trade liberalization and ensuring that a single integrated market was achieved. Unlike the US, the EU imposes controls over business processing and use of personal data, both before and after information is collected.

Two types of privacy laws have been established by various countries to protect privacy[8]:

- Comprehensive laws refer to general laws that govern the collection, use and dissemination of personal information by public and private sectors. The government must consult the body when drawing up new privacy legislation. Examples: European Union, Canada, UK.
- In Sectoral laws, the idea is to avoid general laws and, instead, focus on specific sectors. As in the USA (HIPAA and GLBA)

5 Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground by Avner Levin* and Mary Jo Nicholson†

6 The Council of Europe was established in 1949 in the aftermath of World War II and its horrors, by ten European countries and was charged with the task of strengthening democracy, human rights and the rule of law throughout its member states.

7 Eight basic principles were adopted, providing for collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability of the data collector.

8 International Laws by Ashley Michele Green, Sensitive Information in a Wired World, October 30, 2003

Europe has adopted some directives related to data protection, to consumer protection, electronic signature; and also some initiatives related to Internet security and information society. Each member of the European Union can enforce them on a national point of view

Directives	Content
Data protection	*Directive 95/46/CE issued by the European Parliament and Council on 24 October 1995:* related to the protection of individuals with regard to the processing of personal data and the free movement of such data *Directive 2002/58/CE issued by the European Parliament and Council, 12 July 200:* concerned the processing of personal data and the protection of privacy in the Electronic Communications Sector
Consumer protection	*Directive 85/374/CEE issued by the Council on 25 July 1985*: related to the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products *Directive 91/250/CEE issued by the Council on 14 May 1991: related to the legal protection of computer programs*
Electronic signature	*Directive 1999/93/CE by the European Parliament and Council, 13 December 1999*: related to a community framework for electronic signatures
Internet security	"Create a more secure information society while improving the security of information infrastructures and fighting against cybercrime", one of the first initiatives totally approved by European authorities. It was adopted on 26 January 2001 by the Commission to the Council, the European Parliament, the Economic and Social Committee and the Regions committee"

France has limited legislation. In fact, France only has one data-protection law and one data protection law enforcer: *The Law on Data Processing, Data Files and Individual Liberties (Law No. 78-17)* was enacted in 1978 and significantly amended in 2004. It regulates data processing throughout the economy and throughout government, including the police and national security agencies.

An independent agency, the CNIL is entrusted with extensive enforcement powers. In fact, it is charged with registering and authorizing certain types of data processing operations, with promulgating interpretive regulations, with conducting inspections and imposing administrative sanctions, and with advising the government on legislative and regulatory measures affecting privacy. We will look at its coordination with other organizations within the government in section 7.

3.3. Other foreign laws and regulations

3.3.1.In Japan[9]

To address Information security issues, Japanese Government make considerable efforts. One law related to Information security:

- IT Basic Law, adopted in 2000: *Article 22 – In formulating measures on the construction of an advanced information and telecommunications network society, it is necessary to guarantee safety and reliability of advanced information and telecommunications networks, protect personal information data and implement other necessary measures to ensure that the public can use advanced information and telecommunications networks with a sense of security.*

A framework has been promoted since 2000 with a first Action Plan to protect Information systems against cyber-attacks. E-Japan Strategy II (July 2003) framework included among other requirements, the development of safe and secure IT environment. The next big step was certainly the adoption of "Secure Japan 2006": some priority measures for the information security of the Government of Japan in Fiscal Year (FY) 2006, and the direction for FY 2007[10].

Secure Japan provides an annual plan, the first step toward a Trustworthy Society. For FY 2006, the Government itself sets the priority objective to be the establishment of a system for information security measures in the public and the private sectors. One chapter in this plan discusses the need for all government agencies using a Plan-Do-Check-Act[11] (PDCA) cycle which characterizes an information system security management (ISMS). Having seen the ISMS's approach used by the government, we will not be surprised to see Japan with the highest number of ISMS certifications (ISO 27001). But, we will explain this later during the survey analysis.

Regarding the collection and use of personal information by private parties and public entities, a new Privacy Law establishes fundamental rules and a basic policy. The Privacy Law is intended to set forth fundamental principles for collecting, using, handling and transferring personal information[12].

9 Information Security Policies In Japan by Mabito Yoshida, IT Security Office, MIC, 29 June 2005

10 http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf

11 A simple approach commonly adopted for implementation of ISO27001. It's a cycle designed to be used as a dynamic model, with the end of one turn of the cycle flowing directly into the start of the next, the idea being one of continual improvement

12 http://www.austlii.edu.au/au/journals/PLPR/2003/40.html

3.3.2. In United States[13]

When addressing security at governance and management levels, the following U.S laws along with many others must be considered. They provide regulatory incentives for leaders to pay closer attention to the subject:

Laws	Objective
The U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (also known as Sarbanes-Oxley (SOX))	To mandate expanded public-company financial-control audits, including information security as it relates to the financial reporting process
The U.S. Federal Information Security Act (FISMA) of 2002	To ensure the effectiveness of information security controls over information resources that support federal operations and assets
The U.S. Gramm-Leach-Bliley Act (GLBA) of 1999	To protect personal information for financial-institution customers
The U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996	To protect personally identifiable health information held by certain entities

3.4. Summary

Some laws, regulations or directive address information security management directly; others address it indirectly through such issues as financial governance, privacy or requirements for reporting:

Regulations	France	Global
Internal Control	75%	66%
Protection of personal data	68%	48%
Cryptography use	35%	20%
Protection of Intellectual Property	21%	31%
ISS Certification demands	11%	23%

In France, the government website contains no directive related to information security management. The methods used relate to risk approach (EBios), security policy framework, etc. Actually, one of the main concerns for French organizations is data privacy and protection[14] because of hard sanctions in this area. The regulations in this table above were recorded to affect organizations' information security in 2006. Laws about data privacy and protection are changing the security approach of many organizations. To comply with CNIL's requirements and European directives, organizations have to review among other things, their information systems, and their security practices. Thus, a good security management is needed to facilitate this kind of compliance.

[13] http://www.trustcc.com/resources/glossary/
[14] According an Ernst&Young survey, 2005

In the US, many organizations are more concerned with SOX than with data privacy and protection as Americans don't have the same definition of privacy. But American companies dealing with European one are under the Safe Harbor agreement, the US response to the European directive: "*The Safe Harbor Agreement allows onward transfer of EU data to US companies complying with its requirements, and represents acceptance by the EU Commission of the US Department of Commerce's proposed Safe Harbor Privacy Principles relating to US protection of data privacy insofar as they are applicable to European citizens."*[15]

In Japan, we didn't have a list of laws and regulations addressing security issues. Security management is driven by frameworks and annual plans. The difference with France and US is the commitment of the government in information security management, the use of a managerial approach through the 'PDCA' cycle. Besides this, privacy issues are also regulated like in other jurisdictions.

[15] Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground by Avner Levin* and Mary Jo Nicholson†

4. World Culture

The world is getting smaller and faster, the terms `globalisation′, ′internationalisation′ or `going global′ are key words in our days. This context creates full of confrontations between people since we feel, think and act differently. Geert Hofstede′s as well as Edward T. Hall′s ideas studied cultural problems and pointed out the influence of culture in our day to day life.

4.1. Hofstede's Ideas

Geert Hofstede was born on October 2, 1928 in Harlem, in the Netherlands. He received his Ph.D from Groningen University in 1967. His most famous accomplishment is the distinction of the four dimensions of cultural variability:

- Uncertainty Avoidance

This dimension deals with both: with people's different attitude to time and also with how comfortable people feel towards ambiguity. Uncertainty avoidance can be defined as the extend to which the members of a culture feel threatened by uncertain or unknown situations.[4]

Country	Uncertainty avoidance index
Japan	92
France	86
Spain	86
Turkey	85
Germany	65
United States	46
China	40
UK	35
United States	46

But according to Hofstede, there are societies with low uncertainty avoidance which are characterised by tolerance and moderation. Uncertainty is known and accepted in their daily life and people belonging to such a society deal with unknown risks relatively easy. It is said that such cultures put strong emphasis on Human Rights. Societies with high uncertainty avoidance can be characterised as quite conservative, and intolerant towards unfamiliar religions and ideologies. Detailed rules and laws are to protect them from the unexpected and uncertainty which is part of our every day life is perceived as a permanent threat that has to be opposed. `What is different is dangerous′ is one of the key terms to describe societies with high uncertainty avoidance.

For example, in Germany there is high uncertainty avoidance (65). Germans and French both dislike uncertainty, and thus they try to avoid it. In Germany and France, there is a society that relies on rules, laws and regulations.

- Power Distance

This aspect focuses on the degree of equality or inequality between people in the society of a country. Societies with a high power distance perceive inequality as acceptable. Cultures with a low power distance always try to stress equality and opportunity for everyone.

- Individualism vs. Collectivism

This culture dimension refers to the question of the intensity of interpersonal relationships. According to Hofstede one can distinguish individualistic societies (like France, the USA, the "American dream" is clearly a representation of this) where everybody is responsible for him/herself from the collectivist (like Japan) one where every individual is protected by the group.

- Masculinity vs. Femininity

This aspect focuses on the degree, to which the traditional masculine role model is reinforced in the society. A high masculine ranking indicates a high degree of gender differentiation.

4.2. Hall's Ideas

Edward T. Hall was born on May 16, 1914 in Webster Groves, MO. After receiving his Ph.D. at the Columbia University he spent several years in the U. S. Army Corp of Engineers in Europe. Basically, Hall describes three important aspects of cultural differences paper, two of them:

- High/Low context

This item concentrates on the "amount of information a person can comfortably manage". In high context cultures information is more likely transmitted in non-verbal and indirect ways. Gestures are very important as means of expressing ones opinion. Listeners have to carefully pay attention since important facts have to be read `in between the lines′. Information passes spontaneously and in wide networks. Therefore, the information flow works fast and people tend to be informed on many subjects. Examples of high context cultures: the Arab countries, Japan, France. They tend to be homogenous and collectivist, harmony and saving face are the greatest good; hence, people tend to infer, suggest and imply rather than say things directly.

In low context cultures, information is communicated in a very direct way. Verbalised statements that follow a given plan are usual. This is why the information flow tends to be very slow. Moreover, people tend not to be informed on subjects outside of their own interests. Examples of low context cultures: USA, UK, Germany. They tend to be more heterogeneous and individualist and accordingly have evolved a more direct communication style.

- Monochronic/polychronic cultures

This dimension shows that different cultures have different perceptions of time.

Members belonging to monochronic societies are more likely to have a linear time perception. They are used to doing one item at a time and take time commitments (such as deadlines or schedules) seriously.

On the contrary polychronic societies do not have a linear but rather a cyclic time perception. They do not mind doing several things simultaneously and consider time frames as useful but it does not come to irritations of they cannot achieve them.

In conclusion, it is possible to describe culture as a shared set of basic assumptions and values, with resultant behavioural norms, attitudes and beliefs which manifest themselves in systems and institutions (as well as behavioural patterns and non-behavioural items). So, "*different cultural attitudes will certainly be translated into different regulatory environments" – CSO Magazine, August 2005*. For example, people in Europe, US or Asia will have a different notion of privacy or data protection.

Outside of data protection issues, there tend to be fewer differences in information security, primarily because there are few differences in technical systems: methods of implementing solutions, approach, standards used are different.

Well, the best advice certainly would be not to take Hofstede′s and Hall′s concepts as absolute facts but as tendencies. But, their findings help us understanding that what people do and say in a particular culture are not arbitrary and spontaneous, but are consistent with what people in that culture value and believe in.

5. Perception of Culture

http://www.leadershipcrossroads.com/arti_cwf.htm

"People in France have a different view of how to communicate information. What is said and written in formal communication is often kept to a bare minimum, at least when viewed from an American perspective."

A CSO's Guide to the World – CSO Magazine – August 2005

"A global CSO who assumes that his native country's cultural norms apply to his foreign offices will quickly learn that they do not translate well. If a CSO understand a culture and trusts the professionals working in that culture, he will find it easier to implement policies that meet the spirit of the company's control objectives, and that hold true the world over"

"Europe's history raises its own set of issues. Citizens there tend to have much stricter notions of privacy than Americans, probably because Europeans suffered through the abuses of Nazi and Communist regimes and therefore have higher standards for how personal data can be collected and for what purpose"

Anthony Nelson, IT security consultant & certified information security management systems auditor

"The culture in Japan is to follow the lead of the government, and the government has placed a high importance on ISO 27001 security certification"

"The language spoken determines the point of view, and that point of view does not necessarily translate when you are moving from one language to another"

Paul Raines, Chief Information Security Officer, OPCW, United Nations

"Security can be complex as you enter the international arena. It is essential to take cultural differences into account while managing security in an international environment[16]*"*

Allen, Julia. *Governing for Enterprise Security* (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.

"Security governance and management are most effective when they are systemic, woven into the culture and fabric of organizational behaviours and actions. In this form, it can create and sustain connections among principles, policies, processes, products, people, and performance"

https://buildsecurityin.uscert.gov/daisy/bsi/articles/best-practices/management.html

"This is a tall order, but leaders must be up to the challenge. Their behaviours and actions with respect to security influence the rest of the organization. When staff members see the board and executive team giving time and attention to security, they know that security is worth their own time and attention. In this way, a security-conscious culture can grow. "

[16] http://www.forrester.com/events/agendabyday/print/0,9022,1471,00.html

6. Survey's Details

The study was done in Paris and involved French security professionals. It was designed with two purposes in mind: 1) to bring an answer to the role of culture in managing information security and 2) to find what can facilitate the adoption of ISO 27001 in France and then improve the management of information security.

6.1. About the study

	Survey 1	Survey 2
Objective	- Identify existing laws & regulations that have an impact on security approach - Give a definitive answer to: does culture impact the security approach?	- Identify what slow down the adoption of ISO 27001 in France - List some recommendations to improve the actual situation
Participants	French Security professionals: - M. Gilles Mawas, CISO *Bnp Paribas Group – Banking industry* - M. Thomas Douet, IS Audit Supervisor, Internal Audit *SGICB, Société générale Groupe – Banking industry* - M. Karim Bouherour, Security consultant, Hapsis - M. X, CISO, confidential company in the banking industry - Ms Armelle Trotin, CEO of LSTI *LSTI is the first accredited organization in the field of ISS which can certify and deliver an ISO 27001 security certification.* ***"The views expressed here are theirs and do not reflect the official opinion of their employer or the organization through which the Internet was accessed"***	
Methodology	**Survey instrument** The study consisted of a comprehensive set of questions reviewed by Ron Ruhl, the Director of Concordia Information System Security program. Questions were selected based on their potential to reflect the opinions of experimented people that know French environment related to security. **Collection process:** Once the questionnaire was finalized, the forms were distributed to security professionals in France. Some people respond to the questionnaire via email and others via a conference call. Data collection involved gathering significant qualitative data related to the identified areas. Due to the small number of participants, the results reported herein may not be representative of identified region.	

The banking industry had the greatest participation, in fact the major responding security professional work for international banks based in France. But the study presents significant qualitative data and these data gathered can serve as a vehicle for useful discussion.

6.2. Study Findings and Discussion

6.2.1. Participants' Profiles

Name	Gender	Age	Experience in IT security (years)	Company	Position	Size of the company	Business operations
Armelle Trotin	Female	> 40	>10	LSTI	CEO	<50	Certification authority in the information security area
Gilles Mawas	Male	> 40	>10	BNP Paribas	CISO	>300	Financial institution
Mr X	Male	>40	.5-10	Confidential company	CSO	>50	Clearing House
Thomas Douet	Male	30-35	.2-5	Societe Generale	IS Audit Supervisor	>300	Corporate & Investment Banking
Karim Bouherour	Male	35-40	>10	Hapsis	Manager of the security consulting team	<50	IT Security Consulting and Engineering

This study involves few participants but their contribution was wealthy, collected data are of great quality. These security professionals have experience in IT security. In fact, for many (60%), they work in international organizations which gave to them the mean to interact with people from different cultures using other security approach.

6.2.2. Survey 1

- *Results*

Laws and Regulations that impact organizations in France	**In the following lines, are described some of the laws and regulations that apply to security and identified by participants. They are listed with a brief description of what they encompass.** **- Basel II** *The second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. Basel II is based on three closely linked principles (the "three pillars" concept): a minimum required capital, risk control process and market discipline.* **- CRBF 97-02** *The Committee of Banking and Financial Regulation (CRBF) set «general order regulations applicable to the credit institutions and companies of investment».* *'97-02' refers to one CRBF's regulation established on February 21, 1997. This regulation is related to internal audit and its last version was made applicable by decree in 2005.* **- LSF** *The Law of Financial Security (LSF, also called Law Sea) was adopted by the French Parliament on July 17, 2003 in order to reinforce the legal measures in terms of enterprise governance. Like the American law Sarbanes-Oxley, LSF is based on an increased responsibility of organizations' leaders, a reinforcement of internal audit and a reduction of the sources of interest's conflicts.* **- MIFiD** *The directive involves the market of financial instruments and is one of the last essential parts of the Action plan of financial services. It aims reducing the obstacles to the transborder trade of stocks, facilitating the investment and thus stimulating European economy.* **- Electronic signature (section 4)** **- Cryptography (section 4)** **- Privacy law (section 4)**
Impact of culture	Four among the five security professionals (80%) agreed that culture has an impact on security approach.

- *Analysis*

This section deals with the interaction of the legal system with information security. We have previously presented the main laws/regulations related to security. The findings show us that other regulations impact the security approach in the banking industry more precisely.

Based on the participants' profile, it's obvious that this situation reflects mainly the legal environment in the context of financial markets, banking industry. In fact, developments in computer technology are occurring every day. With every protocol, product or application that is developed, more doors are opened to computer intrusion and misuse. That kind of institutions deal with sensitive data, confidential operations to cover, etc. so they are subject to rigorous regulations like Basel II, Law of Financial Security (LSF), etc. They determine how computer security should be handled in order to be compliant and preserve Information.

Many of these French laws/regulations talk about risks, internal controls, responsibility of leaders (in LSF equivalent to SOX) where the need for a legal system to prosecute perpetrators came. Security is one component of compliance to the banking regulations. Each of these laws and regulations specify some rules and requirements to be respected and implemented at a national and/or European level. As a matter of fact, French central bank and European committees regulate the activities of many local bank and other financial institutions.

Organizations that use the personal information of individuals face the crucial task of maintaining strong controls over personal information. Study results reflect this statement and companies in France have to deal with actual privacy regulations (section 3) to avoid penalties. On a global stage, privacy laws are stricter than those in the US so security professionals have to deal with the context's requirements and adapt their approach to security.

Likewise, organizations have to deal with the restrictions given by video surveillance and cryptography regulations.

In sections 4 and 5, we discussed about culture. Study findings confirm that culture impact security approach. In fact, one company culture is defined by one company's leaders. How people react differ from one country to another. Culture is the key to find the proper security level and it determines people behaviour. As said Ms Armelle Trotin, intellectual property or even privacy is seen differently depending on the countries you are located in (Asia, US, etc.).

6.2.3.Survey 2

Answers from the surveys gave the following results:

- *Results*

Factors that influence the adoption of an ISO 27001 security certification	- Lack of recognition, a total ignorance of what is conformity and certification - Too costly and no French version - Lack of a French 'concrete' participation to ISO sessions - Non-existence of any mandatory statement from the government ; for example in public bids - Non-existence of open spaces where people can access to information for free - Culture at some levels
French government involvement	French government is NOT sufficiently involved in security management. One main reason: - Existence of multiple actors in the government and a bad coordination between them.
Recommendations	- Change the scholar system in France in order to remove the strong split between commercial and engineer paths - Create a benchmark to specify the minimum level of confidentiality to be applied to customer and staff information - Clarify the role of the DCSSI and define one unitary organization to manage security within the government -------- ---------- ---------- - Promote a French version of the standard - Set 'competition' rules to create a triggering element that will encourage managers to get a security certification - Develop and promote the standard via public markets to reach small and average businesses - Involve French insurances to motivate organizations getting a security certification or at least implementing an ISMS - Ask for a security certification in public markets - Lower the cost of security conferences and seminars to attract many people and to advertise the standards, other new security practices and solutions - Develop a strategy in terms of normalization; give means and arguments (from the government) to people representing France during ISO sessions - Prevail upon government subventions as for ISO 9001 quality certification in the past

- *Analysis*

Factors that influence the adoption of an ISO 27001 security certification

In one year, the number of certificates around the world goes from 2200 to 3300. ISO 27001 certificates delivered in Europe:

	End of 2006	**End of 2007**
UK	229	319
DE	56	74
Poland	8	15
France	2	3

For ISO 9001, France recorded 'normal' statistics compared to the global tendency. Qualified ISO 27001 Lead Auditors and organizations that can certify companies exist. Looking ahead, the study respondents cite a variety of obstacles to adoption of this security certification. The most prevalent are cited in the table in the results' section.

Depending on the perimeter you want to certify and other considerations, an ISO 27001 certification can be very costly. Some professionals said that only companies which need it to develop their businesses will go through the burden; others think that budget is not the unique issue. A good organization combined to the awareness of leaders about interests and risks to lower is the key. And the findings show that the adoption of this certification is not only based on business requirements, it's also related to culture as we will see in section 7.

People using Internet or having access to international conferences, national seminars about security via their companies know about the trends and norms in ISM field. But, an overall picture shows us that there is a general lack of recognition of the standard in France. A small part only is aware of the importance of conformity and certification. Another aspect is that the recognition of the certification on the French market is not sufficient for companies to trust that the certification itself is a guaranty of a lower risk. People are not well informed about the perimeters covered by the standards. Participation to security conferences and seminars are costly.

Language is also a barrier; people don't want to be involved into a complex certification process using a 'non-French' version. The characteristics of French culture (high context) will demonstrate that in section 7. There is no French version of the standard. According to Ms Trotin, a French version already exists but it is not official yet, people are currently working on that to make it acceptable by ISO.

In France, people speak English of course but the adequate resources and expertise required for a good implementation of an information security management system (ISMS) depend on an excellent comprehension of the standard. It can help having this standard in French first, to ensure that the approach defined in ISO 27001 is well understand by everyone; second, to make things easy for information security responsible and their leaders and third, to standardize it as it exists a Spanish version.

France like other countries (Germany, UK, Spain, etc.) participates in ISO's work sessions to discuss different topics. One concern highlighted during the study is that security professionals representing France have no recommendations, no watchword vote from the French government itself while other foreign security professionals do.

They have arguments and means to impose themselves during these international meetings with the support of their respective governments. It takes also time and money to participate to the normalization.

One illustration: when ISO 27001 replaced BS 7799/2, France was practically missing during the work session. Once the standard diffused, then professionals have underlined many divergences but it was too late to rectify it.

The fact that there are no regulations or even recommendations to make a security certification mandatory in public bids is also an obstacle. It can be a way to motivate organizations to think about it. Actually, with the new market in Asia, French companies aiming at doing business there must think about this security certification.

About the certificates statistics[17]

Japan	1850
UK	334
India	290
Germany	75
USA	42
Canada	3
France	3

Participants gave their opinion about the statistics above:

Japan has always had a quality approach. We also noticed a cultural effect movement. What motivate companies to get certified can be related to market practices or regulations. People are well-disciplined and they have this formalization approach. For the quality certification, Japan was again among the first countries with a high number of certificates.

United Kingdom (UK) is the 'father' of BS 7799-2 which became ISO 27001 in 2005. Since the terrorism events in London, consideration for good security management has increased.

India holds many outsourcing companies, and we have to revise this certificates number based on the total number of organizations there. To face competition, the certificates are considered as necessary for the IT outsourcing companies.

France's position reflects the little consideration for information security. French banks are using other certification approaches according to Mr Mawas. He said that there are other ways to certify security compliance and it depends on the business line. The domain of economic intelligence might influence the consciousness rising in France, particularly when considering ISM.

French government involvement

The majority of the participants agree that French government can play a better role in security management field. One main reason was identified and will be discussed in section 7.

[17] http://www.iso27001certificates.com/ recent updates can be found at the address

Recommendations for France

Classification of information is one of the most cited recommendations in many security awareness programs. According to Mr. Douet, laws and regulations discuss about all issue except the need for specifying the minimum level of confidentiality to be applied to customer and staff information. This will help define the privacy rules as imposed by the CNIL.

Also, it is recommended that French government specify a benchmark for the minimum level of general security to be applied to the company operations in order to reduce operational risk. Banks are under Basel II which addresses this concern; but with a national benchmark, security professionals would have arguments to ask for resources.

The reorganization of French administration was highlighted by Ms Trotin based on the conclusions given by Pierre Labordes. Mr Labordes is a French representative who did a study involving many public and private organizations during two months and a half. The DCSSI[18] is the department in charge of information systems security and represents the action of French government. The details of this organization are presented in section 7. But, the findings show that there are multiple dispersed services in charge of information security. So there is a need to define one and only one unitary organization to well manage security as the role of the DCSSI is to advice public services, to prepare enterprises' security measures, to ratify security products.

Many participants said that if an institution; say the DCSSI, set some competitiveness rules in the French IT market then it might create a release mechanism. Decision makers within companies will be forced to adhere to market trends if they want to survive and compete with each other.

The results indicate the lack of recognition and advertising of the standard. A way to change this situation is to make chambers of commerce involved. The DCSSI can create some associations via chambers of commerce to hit small businesses and not only big businesses.

Another strategy is to involve insurance companies. One condition to get insurance for a data center for example, will be to hold a security certification or at least implement an information security management system (ISMS). Via public markets also, authorities can set conditions for public bids.

For the sector public, authorities can impose conditions, but what about the private sector? The strategy should not to present the standard as an obligation but serve to influence its adoption. French government can propose internal training, subventions to private companies that want to go into the certification process. The same was done for the certification quality, and it was a success.

According to the Japan Information Processing Development Corporation (JIPDEC)[19], *there is now a trend there is now a trend in Japan of acquiring information security certification quite comparable to earlier trends of certifying business for quality (ISO 9001) and environmental work (ISO 14001).*

---

18 DCSSI: (Central Information Systems Security Division) has succeeded the Central Information Systems Security Division, the State's focal centre for Information Systems Security, and was instituted by decree on 31 July 2001. It is under the authority of the General Secretary for National Defence: http://www.ssi.gouv.fr/en/dcssi/index.html

19 http://www.netpub.se/hotel/itps/4283/html/chapter08.htm

Among the drivers of this trend are the facts that Ministry of Economy, Trade and Industry (METI) maintains an information security management system (ISMS) registration and accreditation scheme for companies working with systems integration and systems operations. Some local governments condition such ISMS certification for procurement. And there is also the factor of peer pressure in the closely knit community of Japanese corporations where the accreditation of one company often requires the accreditation of subcontractors. A final but important reason is the increased focus on information protection and the Personal Information Protection Act of April this year.

Apparently the US companies that are ISMS accredited are those that operate in Japan. In general the US lacks a standard for BS 7799-2 and thus has no certification body. They have other information security management guidelines: *"In the field of information security, cultural differences play themselves out with Europeans being much stronger proponents of ISO 17799 than are Americans, if an American company goes for any type of third-party certification, it is more likely to be a statement on auditing standards (SAS) 70. – CSO Magazine, August 2005"*

In this case, adoption of security standard depends on the business needs there in United States. The trends are not toward an ISO standard. That comes close with the statement of Mr Ron Ruhl which said: *"I believe that business organizations in all countries normally see themselves in a global marketplace, I do not believe that culture will have as big effect as you think. I think it will be more based on business requirements which may include security standards choices and auditing choices"*.

But, Ms Armelle Trotin also argued that during her ISO 27001 certification processes, some companies based on their leaders values, and cultures decided to go through a certification process not because of their business but because of their way of thinking.

7. Theoretical Analysis

7.1. Government's organization around security

The table below presents how countries like US, UK, Germany and France are organized to manage security:

	Information Security agency	Characteristics	Mission	Number of employees (in 2006)
USA	Information Assurance Directorate (IAD), under the authority of the National Security Agency (NSA)	A strong belief: Information Dominance	To provide solutions, products and services, to run protective operations	3000
UK	Communication Electronics Security Group (CESG), under the authority of Communication Government Head Quarter	A developed public and private partnership	To protect and promote the vital interest of the UK and provide assistance on the security of communications and information	450
Germany	Bundesamtfür Sicherheit in der Inf (BSI) attached to Internal Affairs Minister of Germany	A strong product policy more oriented towards users	To inform the country through program awareness for small businesses To provide technical advices and support as part of a strong partnership with the private sector	430
France	Central Information Systems Security Division (DCSSI) under the authority of the General Secretary for National Defence	A stake of national sovereignty	To contribute to Inter-ministerial definition and expression of government policy in terms of information systems security and act as the national regulation authority for ISS	110

Security is everyone problem of course, but government has an important role to play. In France, the DCSSI responsible of security is under the authority of the General Secretary for National Defence (SGDN). In 2005, the budget of the SGDN was 56.7 M€ with a number of employees equals to 353. Only 110 persons are assigned to the DCSSI.

But beyond the SGDN, we have other official actors which develop competences in the field of information security: the Ministry of Defence, the Department for external security (DGSE), the Department of territory supervision (DST), the CNIL, etc. Actually, the DCSSI and the CNIL are working together because the CNIL, on a legal side has more power. Each French ministry has its own approach of security.

Also in France, the regulation in the field of information system security does not exist in the form of a legislative code or lawful code. In fact, as we exposed it in section 3, the field refers to a multitude of texts at very diverse legal levels relating to institutional organization.

According to Mr Labordes, the multiplication of the public actors creates an overlap of mission Unspecified founder legal texts give a general impression of confusion and scattering of means and resources. It is the case for example if we consider certification of products or best practices where the CNIL, the DCSSI and/or other departments intervene at a variable degree of coordination. In this context, the dedicated public actor, the SGDN and more precisely the DCSSI, suffer from lack of authority and sometimes of credibility next to concerned audiences.

Compared to other countries, France uses fewer human resources. The official justification is that there is a lack of qualified ISS specialists within the various administrations, which is particularly alarming for a developed country. If we look at the table, the resources assigned by the counterparts of the DCSSI in other countries are a good indicator of the government priority related to ISS questions. The counterparts develop a true private/public partnership centered on security products. In a general way, it is said that the design and the UK organization of ISS are characterized by a unified approach of both the defensive and offensive aspects of ISS.

Well, on one hand, authorities and regulation institutions influence directly the market. Thus, I think they can play a role to improve the situation and emphasize their influence in this area. On the other hand, the government must be aware of its essential driving role in this particular field of ISSM. Its role should not be limited to a policy of financing and incentives tax.

A way to improve security management can be first to involve small and medium sized businesses (SMB) with the government support as said many security professionals and to adopt and use security standards.

The term of “standardization” holds the image of organization rules imposed by outside which affect the adaptation capacity of companies and their reactivity to market evolution. So, French perceived it as limiting. However, the standards are internationally recognized and they create confidence.

7.2. Role of Culture in this context

In section 4, we have presented two models that deal with culture differences. In summary:

	Context	Individualism	Power Distance	Uncertainty Avoidance
France	High context	High	High	High
Japan	High context	Low	Low	High
US	Low context	High	Low	Low
UK		High	Low	Low

In high-context, a place must be left for adaptation and interpretation. Communication is implicit, informal, symbolic or based on pictures while in low context, they privilege explicit, formal and written communication. Decisions and activities focus often around a central person who has authority

High power distance reveals that the system is autocratic, each member at his place; there is one central authority.

In individualist cultures, we have in-groups and out-groups, individualists emphasize personal goals over in-group goals. In disputes, they are driven more by their personal likes and dislikes and cost-benefits analyses. Individualist cultures value self-reliance and independent thinking.

High uncertainty avoidance relates to a quite conservative culture, intolerant towards unfamiliar religions and ideologies: "what is different is dangerous" is one of the key terms. Rules and structures must be respected.

"People in France have a different view of how to communicate information. What is said and written in formal communication is often kept to a bare minimum, at least when viewed from an American perspective." Section 5

Besides the technical effectiveness of infrastructures, a good security approach depends on the relation you have with key people in an organization: security process to be implemented and reviewed, risks need to be analysed and the need for a good communication between users, leaders and key managers.

Yet, French do not like formal and clear procedures. They want to maintain some form of grey zone and do not want to believe that it is right to use always the same and only way to do the same things. *["French messes rules, the reaction of people is different" Confidential CISO]*

A standard like ISO 27001 is apparently new (Nov 2005) French people need time to adapt. And as located in high context, they tend to be against something which limits their usual tasks. ISO 17799 is used by many French companies, but ISO 27001 talks about something new: the implementation of an Information security management system which imposes a continual review through the PDCA cycle.

High uncertainty avoidance in France reflects the fear for change. What is different is dangerous! If no rule or structure exists, then we don't need to look at it. So, one way to change this behaviour is to put some rules and regulations (imposed by French government) related to security management. Even if it's different, people will at least show an interest. Moreover, as an individualistic culture, in France each member (leader) stresses on personal achievements. We know that leaders' behaviour and values are somehow reflected in the organization management and decisions. So, if there is a rule or regulation about ISO 27001 for example, they will drive the company toward this as leaders focus on success, the success of the company.

For a low context culture like UK, the use of a standard like ISO 27001 will be easier as they are rule oriented and are used to formal and explicit communication (procedures, guides). More knowledge is codified which can explain their creation of series of best practices BS. Also, with a low power distance, there is a strong belief in equality for each citizen. English have the opportunity to rise in society and within their company. It will be easier to involve these people in the organization life: they will be keen to participate to awareness programs for example.

"Europe's history raises its own set of issues. Citizens there tend to have much stricter notions of privacy than Americans, probably because Europeans suffered through the abuses of Nazi and Communist regimes and therefore have higher standards for how personal data can be collected and for what purpose" section 5

Hall adds "high context actions are by definition rooted in the past, slow to change and highly stable". France through the EU has its actions driven by history. Privacy is really important for French people and that's why a high degree in the individualistic dimension was recorded. The key term is 'mind your own business and preserve my privacy'.

"The language spoken determines the point of view, and that point of view does not necessarily translate when you are moving from one language to another" Section 5

While a French version of ISO 9001 was provided, no French version of ISO 27001 exists. But, initially, ISO 27001 was a British standard (BS 7799-2). It's difficult to create a 'friendly' context for the communication; France is in high context where verbal communication is important. People are not familiar with formal communication.

People speak English of course but, based on their culture, the language can be a barrier. The worst can be a bad interpretation of what it is really said. It makes communications difficult, people use to discuss in a foreign language but when it comes to work on an important topic like a security certification with a non-French document trust me, they will not take that risk.

The models of culture described by Hall and Hofstede show that some dimensions of culture might explain why people in some countries think and behave in a certain way while others don't. Based on surveys' findings, some points have been justified but for firm conclusions, more security professionals must be involved with additional survey's questions.

8. Conclusion

This research has given a framework to analyze the influence of culture, laws and regulations on security. This has led to recommendations to be implemented by the French Government in order to encourage companies in France getting a security certification.

This study has shown that some aspects of a country culture as defined by Edward Hall and Geert Hosftede influence information security management. In focusing on the influence of French values, behavior and perceptions on the adoption of ISO 27001, this study demonstrates that there is a relation between security management and culture.

Phone calls interviews and survey questionnaire were used for data collection. Even if the study involved a limited sample of French security professionals, some worth conclusions can be made. Through the examination of regulations and culture influence, concerns with the adoption of ISO 27001 in France, and the role of the French government, the conclusions are summed up namely:

- Hall's and Hosftede's findings gave the means to identify the aspects of French culture: high respect of rules, culture not oriented toward formal procedures and communication, conservative, low capacity for change, fear of uncertainty and individualist.
- Values and perceptions influence the establishment of a regulation. Ex: privacy law differs from one country to another because people didn't have the same vision of privacy. In Europe, thus in France, this notion of privacy is very strong
- French organizations must be more aware of what are conformity, standards and security certification. The collaboration with some institutions like chamber of commerce, insurance's companies can help achieve this. It might be an opportunity to reach small and medium sized businesses and to impose the certification.
- French government must be more involved in security management by first reorganizing its internal authorities in charge of security to end with one unique central authority; second, by reinforcing the position and authority of the DCSSI (Central Information Systems Security Division). Third, based on the Japanese concepts of annual security plan which aims at reaching a 'Trustworthy Society', French government can start defining a model of security that addresses some security management issues, and promoting at least the implementation of an information security management system with a Plan-Do-Check-Act approach.
- French government can encourage companies going through a security certification process with: some kind of subventions for the private sector, the obligation to be certified to access to public market offers (or bids), the establishment of regulations related to information security management.

Information security is interpreted via Culture. The translation and establishment of laws and regulations are affected by Culture. With the progress of technology in the IT field, information privacy must be seriously considered by any organization. Thus, future research is needed to better understand the influence of Culture on privacy perceptions and privacy concerns across different countries. This will help international companies, and security responsible have the means to achieve privacy, to manage security in an effective way.

9. References

URLs

The following links were visited during the research study, between February and April 2007

http://www.xisec.com
http://www.club-iso27001.fr/
http://www.noticebored.com/html/laws.html
http://www.itgovernance.co.uk/page.27001
http://www.iso27001certificates.com/
http://www.oecd.org
http://europa.eu.int/eurlex/lex/LexUriServ
http://www.ssi.gouv.fr/en/regulation/regl.html#crypto
http://www.understandfrance.org/France/Intercultural3.html

Research Papers

Top information security issues facing organizations by Ken Knapp – September/October 2006

A cross-cultural comparison of attitudes towards upward influence strategies by Carolyn Egri, David Ralston

Laws influence business continuity and disaster recovery planning among industries by Kristen Noakes-Fry, Christopher H. Baum, Barry Runyon – July 2005

High/low context, polychronic/monochronic, uncertainty avoidance by Silvia Lechner, 2000

Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground by Avner Levin and Mary Jo Nicholson

Information Systems Security, A Major Stake for France by Pierre Labordes, French Congressman – 26 November 2005

Articles

CSO undercover: Global Security - *A CSO's Guide to the World*, August 2005

An article of Hervé Schauer, a French security specialist who says that *security certification must progress in France*

Secure Japan 2006

Contacts

Ken Knapp, Ph.D in MIS from Auburn University, US

Anthony Nelson, ESTec Systems Corp., Edmonton, Canada

Ed Brownfield, Adjunct Professor - Management Science, C.H.R.P., MSc, 1979, Organizational Development, Pepperdine University

10. Appendices

Collection of personal data

Name	Gender	Age	Experience in IT security (years)	Company	Position	Size of the company	Business operations
Armelle Trotin	Female	> 40	>10	LSTI	CEO	<50	ISO Certification authority in the information security area
Gilles Mawas	Male	> 40	>10	BNP Paribas	CISO	>300	Financial institution
Mr X (Confidential)	Male	>40	.5-10	Confidential company	CSO	>50	Clearing House
Thomas Douet	Male	30-35	.2-5	Societe Generale	IS Audit Supervisor	>300	Corporate & Investment Banking
Karim Bouherour	Male	35-40	>10	Hapsis	Manager of the security consulting team	<50	IT Security Consulting and Engineering

Interviews during conference phone calls:

- Mr X
- Ms Armelle Trotin

Questionnaires filled electronically and received by email

- Mr Gilles Mawas
- Mr Karim Bouherour
- Mr Thomas Douet

Survey 1: About culture, laws and regulations

1. Do you think that French laws and/or regulations impact security approach?

KARIM BOUHEROUR: Respect of CNIL directives, CRBF 97-02, Law of Financial Security, Basel II

GILLES MAWAS: Yes, as a financial institution, we are a regulated industry. Security is one component of compliance to the banking regulations

Confidential: Yes, in the financial industry, some specific regulations exist: CRBS (regulated by Bank of France) 97-02. At a European level, BRI. This determines the context et move people toward a high level of security

THOMAS DOUET: CNIL regulations

ARMELLE TROTIN: There are few regulations in France. No regulation imposes certification, no directive in public bids. Some rules like the Law of Financial Security or Basel II regulate some defined sectors, but overall there is no law aiming at encouraging people to consider security.

2. In your opinion, what role can government play to improve the effectiveness of security approaches used by organizations in France?

KARIM BOUHEROUR: By the implementation of systems for security awareness and for controlling the respect of recommendations and other applicable regulations

GILLES MAWAS: The regulators (governments, Central banks…) should keep on having a risk-based approach, letting the banks explicitly manage their operational risks (including security, compliance, quality…) within a Basel II framework.

CONFIDENTIAL: The ministry of Economy could play a role; the government has no very important role because there are many bodies in place, by ex: the bank of France.

THOMAS DOUET: French government should specify the minimum level of confidentiality to be applied to customer and staff information. It should also specify the minimum level of general security to be applied to the company operations in order to reduce operational risk (it is indirectly included in Basle II, but there is no benchmark).

AT: I think that the government is not very proactive to make taking into account information security. The government has a role naturally, because it makes the laws, proposes subventions and emits public bids. If we take the example of ISO 9000/4, the French government had set up a system of subvention for the companies which decided to go through the certification process. The Department of Commerce wanted to make similar with ISO 27001 by proposing subventions, but only three regions have started to do so and then it stopped. I've proposed to Mr Pierre Labordes to look at this solution again, we are waiting for an action plan.

3. Please give your opinion about the following comments from different security professionals around factors that may influence security approach, mainly the situation in France:

"Culture may influence how organizations implement information systems security"

KARIM BOUHEROUR: Yes

GILLES MAWAS: Yes, obviously, the company culture, as well as the staff behaviour is key in the security awareness and risk management maturity.

CONFIDENTIAL: Yes, culture determines the behaviour of people from a country to the other one. For ex, when we ask to apply a rule:
German applies it without thinking (reflecting), English thinks about it a while but apply, but French messes rules the reaction of people is different. In France it is hard, including security questions.

(With regard to Japan, in France what could be an element release mechanism would be the implementation of rules of competition so that the top management decides to apply the standard 27001 to follow the trends.)

THOMAS DOUET: For each company, the right balance between security and efficiency has to be found. This balance is also a balance between risk management and business development, that is taking place between security (CSO) and control bodies (Regulators, Internal Audit, Risk Managers) and business heads.
Therefore, the culture, and more precisely the experience and awareness of the management, are key to finding the proper security level.

ARMELLE TROTIN: Yes absolutely! The proof BS 7799 is a British standard; when it came out, on certain points it did not correspond to the Latin culture (I mean French culture). In the Latin culture, we ask for evidence, it is necessary to demonstrate things while in the Anglo-Saxon (UK) culture, if you sign, we do not ask you anything else.

Points as intellectual property, private life are differently seen as you are located in Asia, in US or in France. In Asia, if you speak about intellectual property, we look at you with a weird face. They didn't have this notion contrary in France where it is very strong. In the French culture, we do not like all which is certification of conformity, formalized papers, and constraints.

Regarding to the aspect maturity of the standard /// ISO 27001 was published by ISO in October, 2005 but before BS 7799-2 already existed. As proof of that: LSTI made its first certification BS 7799-2 in May, 2005 before the publication of the standard ISO 27001. Otherwise the French version already exists but it is not official, AFNOR is still in expectation. At its release, British Standard (BS) was not very popular in France because she was seen as a British thing, French were more for an international norm. The number of certificates is actually 4 in France

"Culture can lead to a different interpretation of security approach"

KARIM BOUHEROUR: Yes, the missions I've done in one Arab country showed that the approach and interpretation people have about security must be understand in order to succeed in a mission. The way of thinking can be different.

GILLES MAWAS: Yes, there are several ways to solve a business security issue: technology, manual procedures, staff training, avoid doing risky operations…It depends on the industrial sector and on the local / corporate culture.

CONFIDENTIAL: Yes

THOMAS DOUET: Culture is a vague word. I would rather say that the company business strategy is directly or indirectly dictating the security approach. It depends if the company is rather conservative or risk taking.

ARMELLE TROTIN: Look at previous answer

"Regulations and local rules may impact security approach (either those regulations are so rigid that managers allocate more resources and energy to be compliant with them at the expense of effectiveness"

KARIM BOUHEROUR: N/C

GILLES MAWAS: Yes again. One does not do business in New York (under the strict and costy Sarbanes-Oxley mindset) as in Europe or in the Persian Gulf.

CONFIDENTIAL: In France, it is all or nothing. When we make something, we make it well, otherwise we do not make it and we do not even worry about it. The problem is that few ready-to-use solutions exist. Ex, it is difficult and hard to set up a PKI.

THOMAS DOUET: Yes, regulations aim at forcing a minimal level of security in all companies. They push toward stability, by forcing companies to reduce their level of risk.

ARMELLE TROTIN: No comment

Survey 2: About ISO 17799/ISO 27001

4. Are you using ISO 17799 in your company?

KARIM BOUHEROUR: Yes, for our partners and our clients

GILLES MAWAS: Yes

CONFIDENTIAL: Yes and No, because we also work with ISO 13569 (specialized for banking and financial sectors), ISO 17944 (security for banks)

THOMAS DOUET: No, COBIT

ARMELLE TROTIN: Yes, but we use it for our clients

5. Have you heard about ISO 27001?

KARIM BOUHEROUR: Yes

GILLES MAWAS: Yes

CONFIDENTIAL: Yes

THOMAS DOUET: Yes

ARMELLE TROTIN: Yes, we work on it with ISO and AFNOR. We certify companies and people to be 27001 lead auditor

6. Does your company plan to get an ISO 27001 certification?

KARIM BOUHEROUR: Yes, but not soon as we plan to hire more people and create dedicated new branches within the company

GILLES MAWAS: Yes, but in a limited number of business lines, where the investment is needed (for marketing or regulatory reasons)

CONFIDENTIAL: Yes, but in more than 12 months because we have other priorities for the moment and schedule constraints. But ISO 27001 certification is our objective at mid-term.

THOMAS DOUET: No, too costly and not adapted to our environment.

ARMELLE TROTIN: No, because as the organization delivering security certification, we can't ask to be certified by our own people. If one day we need to do it, we will contact an external company.
However, we are under some other norms and regulations.

7. According to you, do you think that it is important for companies to get certified in ISO 27001?

KARIM BOUHEROUR: Yes, to provides high quality of information security management, ISO 27001 is what an organization needs

GILLES MAWAS: It varies greatly from one country to another, from one business line to another. There are other ways to certify security compliance

CONFIDENTIAL: Yes. On a competitive point of view and regarding customers, getting a security certification is very important. As for the quality certification with the standard ISO 9000/4, I think in 5 or 10 years there should be a phenomenon of grouping for ISO 27001.
But there is a problem of mentality and resources. I do not think that the money is a problem, but a good organization, the awareness and the commitment of the leaders to security.

THOMAS DOUET: N/A

ARMELLE TROTIN: Everything depends on the company, some other may not need it. The certification allows the company to cover itself in case of complaints of a customer for example. For service providers: in the case of leak of confidential or personal data, and the customer presses charges against the provider; if the provider is certified (which is equivalent to a good implementation of security practices) he can defend himself in front of a judge and have arguments to demonstrate that his system is fine and that the problem is at another level, not his.
But also, a security certification is a competitive advantage for companies in invitation to tender (public bids). French organizations will have difficulty to position themselves on the international calls for tender without an ISO 27001 certification, ex: contracts in Asia.

To conclude, I think that the certification is important for companies recording high level of risks and those which are thinking about international contracts.

8. What new regulations or changes in regulations in France might improve information security in organizations in France?

KARIM BOUHEROUR: N/C

GILLES MAWAS: Once again, as a bank, we are more impacted by financial / European: International banking regulations (Basel II, MIFiD, FDIC, CRBF 97-02.) then by French laws (Cnil, LSF)

CONFIDENTIAL: There is a regulatory framework which imposes all which is continuity of activities. Because in the employment code, people in charge (say top management) have to ensure business continuity planning. We can think about integrated a section related to security in the employment code that will help increasing the level of security culture in French companies. Crisis plan for bird flu are being implemented.

THOMAS DOUET: N/C

ARMELLE TROTIN: Except the fact of imposing the certification, it would be necessary to make mandatory the implementation of an information security management system for the public administrations. For the private sector, it will be more difficult. But the government can encourage private enterprises to be certified by proposing them subventions, internal training program: an incitement more than an obligation.
Another solution: the insurers have a power which can be more important than that of the government. Under certain conditions, they insure companies. In the field of security certification, why as insurers, they would not impose this certification before accepting any request?

9. Please give your opinion about the following comments from different security professionals:

"*Conformity and certification are not well advertised*"

KARIM BOUHEROUR: Yes, you hear about that in big companies.

GILLES MAWAS: No, not in our business, they are well known

CONFIDENTIAL: Relatively, in France, AFNOR has the role to promote it.

THOMAS DOUET: This may be due to the lack of recognition. The quality of the certifications may not be sufficient for other companies to trust them.

ARMELLE TROTIN: Yes, totally. There is a total misunderstanding of the standard. In France, we do not know what is conformity, certification. People should more participate to conferences and seminar.

"*Adoption of security standards (like ISO 27001) is more based on business requirements; culture has nothing to do with that*"

KARIM BOUHEROUR: N/C

GILLES MAWAS: N/C

CONFIDENTIAL: If all public market regulations impose the certification, we would make a big step. In Japan, people are followers (if you don't do it, you have the label of 'bizarre'. In France, people will put themselves in the process because it will become necessary to preserve business.

THOMAS DOUET: Yes, as it is costly, only companies which need it to develop their businesses will go through the burden. The recognition of the certification on the market is not sufficient for companies to trust that the certification itself is a guaranty of a lower risk.

ARMELLE TROTIN: No, I do not totally agree. Most of companies want to be certified because customers ask them for it, they don't do it for their own. But some companies go through the certification process for their own, they have a proactive attitude. It doesn't depend on their business. They want to be one of the first to be certified, that's it. The company's leaders want it, it's somehow related to the organization culture.

10. The table below is an extract of the number of ISO 27001 certificates per country from www.xisec.com:

Japan	1850
UK	334
India	290
Germany	75
Canada	3
France	3

Please give your opinion about such statistics.

GILLES MAWAS: ISO 27001 was invented in England (BS 7799). Japan has always had a quality approach. French banks are using other certification approaches.

CONFIDENTIAL:
Japan: cultural effect of followers,
UK: historic effect with BS7799-2, the originator of the standards. Besides (to verify! It seems that the British government, particularly armed UK and the subcontractors asks in calls for tender for a certification ISO 27001. There are also the terrorist events in London.
India: with regard to the present companies, '290' can be insignificant
France: Gemalto, one of the 3 has probably get the certification to face international competition.

THOMAS DOUET: In India, the certificates are considered as necessary for the IT outsourcing companies. There is probably a similar reason in UK and Japan: either market practices (for service providers) either regulation.

ARMELLE TROTIN: France: it's pity, it shows the level of security awareness in France. It reflects the low interest for security.
Japan: people are very disciplined, they have this notion of formalization. With ISO 9000, Japan still was among the first having the quality certification.

11. What do you think about French government's implication in Information security field?

KARIM BOUHEROUR: Can do better, its has a low profile in this domain

GILLES MAWAS: Adequate

CONFIDENTIAL: In public bid (calls for tenders), there is no obligation to be ISO 27001 certified. The historic use of the DCSSI can be a brake because in the past, this body had a military activity. Thus people do not feel really concerned. Government should do something to first let people know the roles of the DCSSI and give it authority.

THOMAS DOUET: French government and companies are less IT oriented than UK / US or even Japan. For most of them, IT is rather a difficulty, than a success tool. For IT security, it is even worse!

AT: Its role is not sufficient and the DCSSI has no resources. Like said Mr Pierre Labordes, we have a multitude of organizations within the government and dealing with security. They don't communicate between them, so they are not effective. Also, there is a lack of advertising, and the non-existence of places where people can get information for free. *(one recommendation from me which was approved by ms Trotin)*

There is also a lack of participation to the standardization (because it takes time and money to participate to ISO sessions). What slows down companies, they do not know about novelties, tendencies. When the BS 7799 went out as ISO 27001, France being almost absent during its elaboration underlined points of differences.

12. Please give your recommendations to improve the situation

KARIM BOUHEROUR: More involvement of the DCSSI

GILLES MAWAS: We believe that the situation is fine in the European financial sector and we do not recommend any improvement.

CONFIDENTIAL: Promote the standard in French, develop it via public market, try to make extracts by domain of activity. The DCSSI has to create associations with chambers of commerce so that they touch small and medium sized firms and promote the standard.

THOMAS DOUET: Change the scholar system in France, in order to remove the strong split between commercial and engineer paths.

AT: The government has a role to play, he has to define the strategy in terms of standardization, a strategy that have English, German, etc. During the ISO meetings regrouping many countries representatives, The French people receive no order of vote, no suggestion from the government. My colleagues compared to other have very little means, very few arguments to say and impose any needs to add this, develop that, etc. French government has to be more involved.

13. Add any other comments you want to spotlight in this study

CONFIDENTIAL: In France, there is a time to adapt and assimilate security culture (about 2 years). We must also think about the maturity cycle of ISO 27001 since its release in 2005. Where France is located in this cycle?

11. Approved Research Proposal

Table of Content

1. Personal Information

Mame Gnagna Diop
3, avenue de Verdun
92250 La garenne colombes
France

Personal Phone : +336 65 30 59 36

Email : mgdiop@gmail.com

2007: Master of Information System Security Management – Concordia University College of Alberta (Canada), pending status on Research completion

2006: Engineer degree in Network and Information systems – Ecole Centrale d'Electronique de Paris (ECE) (France)

2001: Degree of computing in a vocational higher education college – Ecole Supérieure Polytechnique de Dakar (Senegal)

1999: French Scientific Baccalaureate with honors, speciality in mathematics equivalent to A level

2. Research Title

Ways to improve information security management in France:
Impact of culture regulations, role of the government

3. Research Statement

What are the factors that influence the management of information security in France?

4. Proposed Research Advisors

Primary advisor: Ron Ruhl, Director
Information Systems Security Program and Assistant Professor of Management
Faculty of Professional Education
Gold Bar Campus
Concordia University College of Alberta
E-mail: rruhl@concordia.ab.ca
Phone: 780-413-7822
Fax: 780-466-9394

Secondary advisor: Dr. Pavol Zavarsky, Director of Research
Information Systems Security Program and Associate Professor
Faculty of Professional Education
Gold Bar Campus
Concordia University College of Alberta
E-mail: pavol.zavarsky@concordia.ab.ca
Phone: 780-413-7810
Fax: 780-466-9394

5. Abstract

Considering that many organizations today are fully dependent on information technology for survival, information security is one of the most important concerns facing the modern organization. According to Paul Raines, CISO, OPCW, United Nations, '*Security can be complex as you enter the international arena. It is essential to take cultural differences into account while managing security in an international environment*[20]' *Paul Raines, Chief Information Security Officer, OPCW, United Nations*
This study attempts to reveal some of the impact of culture, regulations on security approach; and also why a security certification is not well adopted in French companies in opposition to other countries like Japan or US. The central objective is also to give an answer to what many security professionals agree (or not) that culture and local rules/regulations are something we have to deal with in order to preserve security.

[20] http://www.forrester.com/events/agendabyday/print/0,9022,1471,00.html

6. Outline

Introduction

1- Information Security Management (ISM)
    What is ISM? Definition of people around the world

2- ISO Standards *(quick presentation, statistics about their adoption, etc.)*
    a. ISO 17799
    b. ISO 27001

3- Laws & Regulations related to Information Security
    a. French
    b. European
    c. Other: Canada, US, Japan

4- World Culture *(a general presentation of cultural norms, society, etc. around the world that will be benefit in section #7)*

5- Perception of culture *(write some numbered paragraph including some statements that will help later in discussion or during analysis)*

6- Surveys Details
    a. Survey 1:
        - Objective
        - Participants
        - Methodology
        - Results
        - Analysis

    b. Survey 2:
        - Objective
        - Participants
        - Methodology
        - Results
        - Analysis

7- Theoretical Analysis
    US, Japan, Europe (France): Comparison between information security management, standards used, approach to security

8- Conclusion
    a. Recommendations based on participants' feedbacks
    b. Direction for future research (?)

7. Disciplinary Context

Complex information system security today focuses on the design of safe and secure information systems and their operations. But, some other aspects must be taken into account because technology alone cannot lead to an adequate solution. Culture, local rules and regulations influence security approach and as stated in a Global security article (CSO website), different cultural attitudes translate into different regulatory environments.
While some people agree that these factors also influence the security approach and the adoption of standards, others totally disagree.

8. Methodology

The aim of the research project is to collect information about security management in French companies (looking at culture and regulations), and also the factors that hold back the adoption of a standard like ISO 27001 and to see how French government can help improving the situation.

The study will be a qualitative research (interviews, surveys) involving collection, discussion rather than manipulation. All the findings will be mainly summarized as text rather than statistics.

The study involves information systems security professionals and will be pursued namely:

1- Make a first survey to find out:
   a. If any actual French/European law and/or regulation is seen as a problem to security management,
   b. The place of culture in managing information security and its influence to security approach
   c. Their opinion about some hypothesis that will help during the theoretical analysis

2- In a follow-on survey, they will
   a. Give their opinion on ISO 27001
   b. Discuss some reasons why such security certification is not well adopted in France.
   c. Then, survey participants will discuss the participation of French government in this environment.

   In this part, we will include the participation of security responsible from some French ministries in order to know their perception of a security certification.

Then, a theoretical analysis based on literature, articles, and general opinions will be done.

My objective is to end up with an analysis (based on results and also general comments) of collected information, to detect cultural/regulatory impacts that can explain some points and frequent recommended government actions will be summarized.

9. Review of Existing Research

I didn't found any existing research directly related to this subject, but many articles discussed the impact of culture (Ex: CSO undercover: Global Security - A CSO's Guide to the World), in other studies and findings (Ex: EY), we always find the issue of laws, regulations on information security.

On the other hand, many French specialists (Ex: Herve Schauer, Mauro Israel) debate on the fact that security certification is not well considered in French companies. Why? Lack of budget? Lack of advertising?

So, we have many opinions but not a real explanation based on concrete statements. The paper 'Top information security issues facing organizations' by Ken Knapp develops the role of US government to help improving security issues. This led me explore in this study the role of French government.

10. Contribution to Knowledge

For foreign practitioners understanding and then adhering to local culture and customs can avoid compromising security. It will give essence to future debates about culture between people. Comments of French security professionals about the role of the government will give a public opinion; comparison with other countries also can point some areas to improve.

For researchers, the results of these surveys can be valuable from an educational perspective because the same can be done in other countries.

11. Preliminary Bibliography

The main ressources I'm using concern the following:

URL:

(1) http://www.xisec.com

(2) http://www.club-iso27001.fr/

(3) http://www.noticebored.com/html/laws.html

(4) http://www.itgovernance.co.uk/page.27001

Books:

(5) Information on comparative laws: Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Ithaca: Cornell University Press, 1992)

Articles:

(6) CSO undercover: Global Security - A CSO's Guide to the World, August 2005

(7) An article of Hervé Schauer, a French security specialist who says that security certification must progress in France

Research Papers:

(8) 'Top information security issues facing organizations' by Ken Knapp – September/October 2006

(9) A cross-cultural comparison of attitudes towards upward influence strategies by Carolyn Egri, David Ralston

(10) Laws influence business continuity and disaster recovery planning among industries by Kristen Noakes-Fry, Christopher H. Baum, Barry Runyon – July 2005

(11) Information Systems Security, A Major Issue for France by Pierre Labordes, French Congressman – 26 November 2005

Contacts:

And also, I have comments by email from:

Ken Knapp, Ph.D in MIS from Auburn University, US

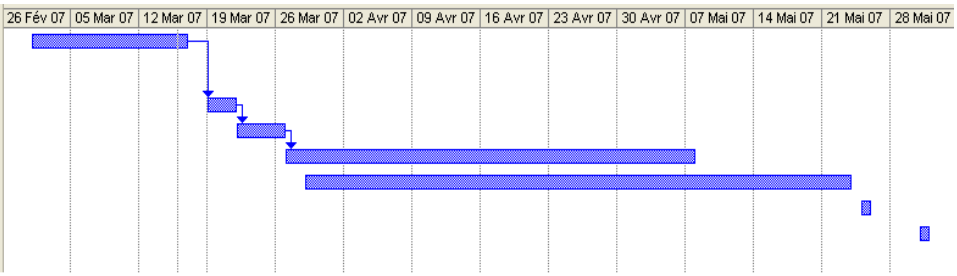
Anthony Nelson, ESTec Systems Corp., Edmonton, Canada

Mauro Israel, ISO 27001 Lead auditor, CyberNetworks, Paris, France

12. Research Schedule

The following schedule was done with a French version of MS Project, but I will send an English version as soon as I get back my laptop. Well, it's a way to make you learn French ☺

Nom de la tâche	Durée	Début	Fin
Proposal Writing & Submission to committee	12 jours?	Jeu 01/03/07	Ven 16/03/07
Proposal Validation	3 jours	Lun 19/03/07	Mer 21/03/07
Proposal Review	3 jours	Jeu 22/03/07	Lun 26/03/07
Surveys' collection	30 jours	Mar 27/03/07	Lun 07/05/07
Writing paper	40 jours	Jeu 29/03/07	Mer 23/05/07
Paper submission	1 jour	Ven 25/05/07	Ven 25/05/07
Paper presentation	1 jour	Jeu 31/05/07	Jeu 31/05/07



Jeu 01/03/07 *means* Thurs 03/01/07
Jours *means* days
Durée *means* duration
Début *means* start
Fin *means* end

The submission to committee is on Friday 03/16/07, after the validation and a complete review planned on Mon 03/26/07, I will start the surveys' collection (duration=30 days). During this collection period, I will start the writing of the research paper in order to present it on Thurs 05/31/07.